UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,946	01/19/2000	Bjorn Markus Jakobsson	Jakobsson 13-1	3763

27550 7590 10/27/2003

WALTER J, TENCZA JR.
10 STATION PLACE, SUITE 3
METUCHEN, NJ 08840

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	3

DATE MAILED: 10/27/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/487,946	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-8 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-8 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 19 January 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 3 and 4 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claim 3 and 4 recites the limitation "the encryption steps". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier Applied Cryptography 2nd Edition (hereinafter Schneier). As per claim 1, Schneier teaches an

ElGamal encryption method which substantially covers the claim (see Schneier, page 478, 'ElGamal Encryption'). Although the method disclosed by Schneier is silent on the matter of encrypting a key value (the ElGamal scheme is taught as a method to encrypt a general message), it is conventional in the art to use public key encryption methods for secure key exchange, especially those that are variants of the Diffie-Hellman key exchange algorithm. Also conventionally known is that public key encryption methods are much slower and generate a longer ciphertext than symmetric methods (but they provide a more secure ciphertext based on similar key lengths); hence, message encryption is typically divided into two work loads: a public key encryption method is used to exchange a session key whereupon a symmetric algorithm using this session key encrypts the message (see Schneier, page 216, 'Public-Key Cryptography verses Symmetric Cryptography'). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to use the ElGamal encryption method as disclosed by Schneier to securely transmit a secret key from a sender to a receiver for the purpose of encrypting and decrypting a message with the secret key. The motivation for such an implementation would enable a faster cryptosystem for the secure transmission of messages. Hence, the ElGamal encryption method comprises the steps of:

a. encrypting a message M using a primary secret key z to form a quantity E;

b. encrypting a session key z by preparing:

   i. a(new) = z*y^c modulo p;

   ii. b(new) = g^c modulo p;

   where y = g^x modulo p, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method;

c. decrypting a(new) and b(new) using the receiver secret key x to get the primary secret key z;

d. using the primary secret key z to decrypt the quantity E and obtain M

(see Schneier, pages 478, 'ElGamal Encryption'; pages 513-515, 'Diffie-Hellman'). This encryption method disclosed by Schneier does not specify the step of generating a signature based on the triplet a(new), b(new) and E. However, as disclosed by Schneier in a separate section, signing documents is the standard methodology to ensure the identity of the author of a message and to verify the integrity of the message (see Schneier, pages 34-44, 'Digital Signatures', 'Digital Signatures with Encryption'). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to generate a signature s(new) as a function of a(new), b(new), and E by the sender and have the receiver of the transmission validate the signature. Motivation for this combination would enable the invention to implement a more secure transmission methodology. Hence, the aforementioned covers claim 1.

7. As per claim 2, Schneier covers an ElGamal encryption method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the step of decrypting a(new) and b(new) using the receiver secret key x to get the primary transmitter secret key z is comprised of computing z = a(new)/b(new)^x (see Schneier, page 478, 'ElGamal Encryption').

8. As per claims 3 and 4, Schneier covers an ElGamal encryption method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, ElGamal encryption is used for the encrypting steps (see Schneier, pages 476-479, section 19.6).

9. As per claim 5, Schneier covers an ElGamal encryption method as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). Schneier is silent on the matter of defining a function to determine the value of z. However, the members of the set Z = {g^k modulo p | k is a nonnegative number} are obvious candidates since this set would enable the value z*y^c modulo p to be a member of the group G modulo p generated by the generator g of order @(p), where g and p are relatively prime, @() is Euler's totient function, and g^@(p) = 1 modulo p. Since:

z*y^c modulo p = (g^k modulo p * g^(x*c) modulo p) modulo p

= g^(k+x*c) modulo p.

a(new) is a one to one function of k given that 0 <= k+x*c <= @(p), where x and c are held constant. Hence, using the aforementioned constraints, the sender can be confident that distinct values of k will generate distinct primary transmitter secret keys z. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to generate the primary transmitter secret key from the formula z = g^k modulo p, where k is a random value chosen from the set [0...q], where q is a value picked using a known encryption method.

10. Claims 6, 7, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier as applied to claim 1 above, and further in view of admitted prior art as disclosed by the applicant in the specification (hereinafter admission). As per claims 6 and 7, Schneier covers an ElGamal encryption method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Schneier is silent on the matter of defining 2 private transmitter keys z and z' where z' = f(z) for some function f() and z' is the key which encrypts and decrypts the message M. However, as

disclosed by admission, it is conventional in the art to use functions, such as truncation, to modify a generated key value to be used in an encryption method that requires a different key length (see admission, page 12, line 14 – page 13, line 3). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to define a second private transmitter key z', where z' = f(z) for some function f() and z' is the key used to encrypt and decrypt the message M, when the primary transmitter key z is provided and is not of the format used for producing the ciphertext E. The motivation for such an implementation would enable the invention disclosed by Schneier to implement a function to encrypt message M that is independent (or at least less dependent) of the function that generated the first primary transmitter key z. This independence enables the cryptosystem to be designed with functions based more on security benefits than on compatibility issues.

11. As per claim 8, Schneier covers an ElGamal encryption method as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). In addition, admission discloses providing a plurality of portion keys which are derived from the secondary transmitter key z' and the plurality of portion keys encrypts and decrypts a data message m when the secondary transmitter key z' is provided which is not of the format used for producing the ciphertext E (see admission, page 12, line 14 – page 13, line 3).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Hellman et al. U.S. Patent No. 4,200,770 discloses a cryptographic apparatus and method.

Crandall et al. U.S. Patent No. 5,271,061 discloses a method and apparatus for public key exchange in a cryptographic system.

Dwork et al. U.S. Patent No. 5,539,826 discloses a method for message authentication from non-malleable crypto systems.

Zheng U.S. Patent No. 6,396,928 discloses a digital message encryption and authentication.

Jakobsson U.S. Patent No. 6,507,656 is the parent application of the current application.

Dolev et al. 'Non-Malleable Cryptography' defines the non-malleable property and offers several non-malleable schemes.

Crescenzo et al. 'Non-Interactive and Non-Malleable Commitment'.

ElGamal 'A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms'.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jung W Kim
Examiner
Art Unit 2132

jk
October 9, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100